UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/616,100	07/08/2003	David P. Cook	10664-130002	1883

26181   7590   09/10/2007

FISH & RICHARDSON P.C.
PO BOX 1022
MINNEAPOLIS, MN 55440-1022

EXAMINER
NGUYEN, MINH DIEU T

ART UNIT	PAPER NUMBER
2137	

MAIL DATE	DELIVERY MODE
09/10/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

PTOL-90A (Rev. 04/07)

	Application No.	Applicant(s)
Office Action Summary	10/616,100	COOK, DAVID P.
	Examiner	**Art Unit**	
	Minh Dieu Nguyen	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) OR THIRTY (30) DAYS,
WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _18 June 2007_.

2a)☒ This action is **FINAL**.   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _93,94 and 97-107_ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _93-94 and 97-107_ is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All   b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☐ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.

5)☐ Notice of Informal Patent Application

6)☐ Other: _____.

DETAILED ACTION

1.   This office action is in response to the communication dated 6/18/07 with the amendments to claims 93, 97-101 and 103-107.

2.   Claims 93-94 and 97-107 are pending.

Response to Arguments

3.   Applicant's arguments filed 6/18/2007 have been fully considered but they are not persuasive. Applicant argues that Daniels' reference does not teach providing a list of recipients, in particular, the control information does not specify any intended recipient. The examiner respectfully disagrees, Daniels discloses a mass mailing delivery mechanisms, in particular, combined electronic and physical delivery mechanisms (Daniels: col. 1, lines 5-7) with documents, as specified in the addressing information, to a physical address and documents are to be delivered via an electronic mail, as specified in the preferences (Daniels: col. 3, lines 43-55). It is inherently understood in order for a document to be delivered either through a physical delivery or electronic delivery, the recipients' addresses need to be provided, in other words, a list of recipients is given.

On page 10 of the remarks, Applicant alleges the Examiner admitted Daniels does not disclose these features (i.e. decrypting a received encrypted message at the forwarding server and **determining a delivery preference** for each recipient) and Kobata does not teach determing a delivery preference. The Examiner suggests

Applicant reviews the previous office action, in particular, page 4, wherein Examiner indicated that Daniels is silent on the capability of decrypting the encrypted message at the forwarding server and re-encrypting the message. However, Daniels clearly discloses determining a delivery preference as addressed in detail in the previous office action.

Applicant argues that Owens does not teach notifying a recipient that a message is available for retrieval if a delivery reference has not been specified by the recipient and further Applicant submits that Owens teaches away from the claimed invention. The Examiner respectfully disagrees, both Daniels and Kobata disclose notifying a recipient when the message is available for retrieval (Daniel: col. 4, lines 18-23; Kobata: col. 5, lines 43-46), Owens indicates that if the message receiver does not specify a preference for receiving the incoming message, the incoming message will be forwarded to receiver's mailbox, to another electronic mailboxes or to the Internet (Owens: col. 5, lines 37-44) for later retrieval (Owens: col. 4, lines 18-20; col. 6, lines 52-55). Owens does not teach away from the claimed invention because the claimed language does not particularly recite that the message can not be stored in the receiver's mailbox for later retrieval.

Applicant argues that Jones does not determine the decryption capability of the user device and Examiner uses Applicant's claims as hindsight reconstruction. The Examiner respectfully disagrees, Jones discloses determining the decryption capability of the user device as such it depends on the user device, there are different ways of

protecting/encrypting the information (i.e. different decryption capability) Jones: col. 4, line 30 to col. 5, line 45).

In response to applicant's argument that the examiner's conclusion of obviousness is based upon improper hindsight reasoning, it must be recognized that any judgment on obviousness is in a sense necessarily a reconstruction based upon hindsight reasoning. But so long as it takes into account only knowledge which was within the level of ordinary skill at the time the claimed invention was made, and does not include knowledge gleaned only from the applicant's disclosure, such a reconstruction is proper. See In re McLaughlin, 443 F.2d 1392, 170 USPQ 209 (CCPA 1971).

Applicant argues that Bengtsson does not suggest re-encrypting a decrypted message according to a decryption capability of a recipient.

In response to applicant's arguments against the references individually (i.e. Bengtsson), one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See In re Keller, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); In re Merck & Co., 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

Applicant argues that the word "encryption' or "decryption" does not occur at all in the description of Bengtsson. The Examiner respectfully disagrees, the sending party send the text portion of the SMS message to the receiving party via an SMS server, while the attachment is transmitted to a different server (Bengtsson: col. 5, lines 22-34), when the receiving party does not have a decryption capability (i.e. no capability to

decipher, the server will deliver in a format that is understood by the receiving terminal,

so the receiving terminal could download the information easily (Bengtsson: col. 5, lines

43-55).

Claim Rejections - 35 USC § 103

4.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

5.   Claim 93 is rejected under 35 U.S.C. 103(a) as being unpatentable over Daniels,

Jr. et al. (6,343,327) in view of Kobata et al. (7,051,003).

Daniels discloses a computer implemented method for sending a secure

message to multiple recipients (i.e. a system and method for electronic and physical

mass mailing, see Daniels: col. 1, lines 5-7) comprising: encrypting a message (i.e.

printstream processor 102 may encrypt the documents with a content encryption

processor, see Daniels: col. 3, lines 53-55), sending the encrypted message to a

forwarding server (i.e. the encrypted information is forwarded to the message router,

see Daniels: Fig. 1, element 112), including providing a list of recipients to the

forwarding server (i.e. Daniels discloses a system for mass mailing delivery with

addressing information in the form of delivery preferences for each recipients, see

Daniels: Fig. 1, element "Control Info. And References"; col. 4, lines 46-49); at the

forwarding server, determining a delivery preference for each recipient in the list of

recipients (i.e. message router decodes the delivery preference data, see Daniels: col.

6, lines 66-67); and for each recipient that has a delivery preference, delivering the

message in accordance with the delivery preference (i.e. the message router delivers

the electronic mail pieces via an electronic delivery mechanism specified in the delivery

preferences, see Daniels: col. 2, lines 14-17).

Daniels is silent on the capability of decrypting the encrypted message at the

forwarding server and re-encrypting the message. Kobata is relied on for the teaching of

decrypting the encrypted message at the forwarding server, re-encrypting the message

and delivering the re-encrypted message (i.e. a server system is connected to the

network to receive the encoded document, the server system comprises a processor

that executes decryption software to decode the document encoded by the sending

system and executes encryption software to encode the decoded document before

delivering the document, see Kobata: col. 2, lines 40-46).

It would have been obvious to one of ordinary skill in the art at the time of the

invention to employ the use of decrypting the encrypted message at the forwarding

server, re-encrypting the message and delivering the re-encrypted message in the

system of Daniels, as Kobata teaches so as to provide security of the outgoing

electronic mail piece (see Daniels: col. 4, lines 23-25).

6.   Claims 94 and 97-99 are rejected under 35 U.S.C. 103(a) as being unpatentable

over Daniels, Jr. et al. (6,343,327) in view of Kobata et al. (7,051,003) in view of Owens

et al. (6,023,700)

a)   As to claim 99, the combination of Daniels and Kobata discloses the

method of claim 93, further comprising notifying each recipient that the message is

available for retrieval (i.e. the sending system notifies the receiving system of the

imminent delivery of a parcel, see Kobata: col. 5, lines 43-46). However the combination

of Daniels and Kobata is silent of the capability of (notifying) each recipient that does

not have a delivery preference. Owens is relied on for the teaching of (notifying) each

recipient that does not have a delivery preference (i.e. if the message receiver does not

specify a preference for receiving the incoming message, the incoming message will be

forwarded to one or more electronic mailboxes (for later retrieval), see Owens: col. 5,

lines 37-44). It would have been obvious to one of ordinary skill in the art at the time of

the invention to employ the use of (notifying) each recipient that does not have a

delivery preference (that the message is available for retrieval) in the system of Daniels

and Kobata, as Owens teaches, so as messages are delivered in accordance with the

preferences of the senders and receivers (see Owen: Abstract).

b)   As to claim 94, the combination of Daniels, Kobata and Owens discloses

the method of claim 99, wherein notifying the recipient includes notifying the recipient

that the message is available for retrieval through a secure link (i.e. the retrieval can

require log-on authentication such as username and password to retrieve message, see

Kobata: col. 6, lines 34-45).

c)   As to claim 97, Daniels discloses a computing system for providing secure

message services for messages addressed to multiple recipients (i.e. a system and

method for electronic and physical mass mailing, see Daniels: col. 1, lines 5-7)

comprising: a forwarding engine (i.e. message router, see Daniels: Fig. 1, element 112)

executing on a computer operable to: receive an encrypted message and a list of

recipients (i.e. printstream processor 102 may encrypt the documents with a content

encryption processor, see Daniels: col. 3, lines 53-55, the encrypted information is

forwarded to the message router, see Daniels: Fig. 1, element 112, Daniels discloses a

system for mass mailing delivery with addressing information in the form of delivery

preferences for each recipients, see Daniels: Fig. 1, element "Control Info. And

References"; col. 4, lines 46-49); determine a delivery preference for each recipient in

the list of recipients (i.e. message router decodes the delivery preference data, see

Daniels: col. 6, lines 66-67), for each recipient that has a delivery preference, delivering

the message in accordance with the delivery preference (i.e. the message router

delivers the electronic mail pieces via an electronic delivery mechanism specified in the

delivery preferences, see Daniels: col. 2, lines 14-17).

Daniel is silent on the capability of decrypting the encrypted message, re-

encrypting the message and delivering the re-encrypted message. Kobata is relied on

for the teaching of decrypting the encrypted message, re-encrypting the message and

delivering the re-encrypted message (i.e. a server system is connected to the network

to receive the encoded document, the server system comprises a processor that

executes decryption software to decode the document encoded by the sending system

and executes encryption software to encode the decoded document before delivering

the document, see Kobata: col. 2, lines 40-46).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of decrypting the message, re-encrypting the message and delivering the re-encrypted message in the system of Daniels, as Kobata teaches so as to provide security of the outgoing electronic mail piece (see Daniels: col. 4, lines 23-25).

Kobata further discloses notifying each recipient that the message is available for retrieval (i.e. the sending system notifies the receiving system of the imminent delivery of a parcel, see Kobata: col. 5, lines 43-46). However the combination of Daniels and Kobata is silent of the capability of (notifying) each recipient that does not have a delivery preference. Owens is relied on for the teaching of (notifying) each recipient that does not have a delivery preference (i.e. if the message receiver does not specify a preference for receiving the incoming message, the incoming message will be forwarded to one or more electronic mailboxes (for later retrieval), see Owens: col. 5, lines 37-44). It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of (notifying) each recipient that does not have a delivery preference (that the message is available for retrieval) in the system of Daniels and Kobata, as Owens teaches, so as messages are delivered in accordance with the preferences of the senders and receivers (see Owen: Abstract).

d)   As to claim 98, the combination of Daniels, Kobata and Owens discloses the method of claim 97, wherein the forwarding engine is operable to: notify the recipient that the message is available for retrieval through a secure link (i.e. the

retrieval can require log-on authentication such as username and password to retrieve

message, see Kobata: col. 6, lines 34-45).

7.   Claims 100 and 103-105 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Daniels, Jr. et al. (6,343,327) in view of Kobata et al. (7,051,003) in

view of Jones et al. (6,697,944).

        a)   As to claim 100, Daniels discloses a computer implemented method for

sending a secure message to multiple recipients (i.e. a system and method for

electronic and physical mass mailing, see Daniels: col. 1, lines 5-7) comprising:

encrypting a message (i.e. printstream processor 102 may encrypt the documents with

a content encryption processor, see Daniels: col. 3, lines 53-55), sending the encrypted

message to a forwarding server (i.e. the encrypted information is forwarded to the

message router, see Daniels: Fig. 1, element 112), including providing a list of

recipients to the forwarding server (i.e. Daniels discloses a system for mass mailing

delivery with addressing information in the form of delivery preferences for each

recipients, see Daniels: Fig. 1, element "Control Info. And References"; col. 4, lines 46-

49); delivering the message to the recipient (i.e. the message router delivers the

electronic mail pieces, see Daniels: col. 2, lines 14-17).

        Daniels is silent on the capability of decrypting the encrypted message at the

forwarding server, determining a decryption capability for each recipient in the list of

recipients and for each recipient, re-encrypting the decrypted message according to the

decryption capability of the recipient. Kobata is relied on for the teaching of decrypting

the encrypted message at the forwarding server, re-encrypting the decrypted message

and delivering the re-encrypted message to the recipient (i.e. a server system is

connected to the network to receive the encoded document, the server system

comprises a processor that executes decryption software to decode the document

encoded by the sending system and executes encryption software to encode the

decoded document before delivering the document, see Kobata: col. 2, lines 40-46).

It would have been obvious to one of ordinary skill in the art at the time of the

invention to employ the use of decrypting the encrypted message at the forwarding

server, re-encrypting the message and delivering the re-encrypted message in the

system of Daniels, as Kobata teaches so as to provide security of the outgoing

electronic mail piece (see Daniels: col. 4, lines 23-25).

The combination of Daniels and Kobata is silent on the capability of determining

a decryption capability for each recipient in the list of recipients and (re-encrypting) the

decrypted message according to the decryption capability of the recipient. Jones is

relied on for the teaching of determining a decryption capability for each recipient in the

list of recipients and (re-encrypting) the decrypted message according to the decryption

capability of the recipient (i.e. digital content is encrypted and transmitted to each

portable player device according to the decryption capability of each portable player

device, see Jones: col. 4, lines 30-35).

It would have been obvious to one of ordinary skill in the art at the time of the

invention to employ the use of determining a decryption capability for each recipient in

the list of recipients and (re-encrypting) the decrypted message according to the

decryption capability of the recipient in the system of Daniels and Kobata, as Jones

teaches, so as to ensure proper protection of the transmitted data (see Jones: col. 1,

lines 8-14).

b)   As to claim 103, the combination of Daniels, Kobata and Jones discloses

the computer implemented method of claim 100, wherein determining a decryption

capability for each recipient includes determining whether each recipient has an

associated published key (i.e. each portable player device has an associated public key

where the digital content is encrypted using the public key so that the portable player

device is able to decrypt the digital content using its associated private key, see Jones:

col. 4, lines 30-35).

c)   As to claim 104, the combination of Daniels, Kobata and Jones discloses

the computer implemented method of claim 100, wherein determining a decryption

capability for each recipient includes determining whether each recipient has an

associated certificate (i.e. each portable player device has an associated digital

certificate and needs to present the digital certificate prior to receiving the digital

content, see Jones: col. 10, lines 28-32).

d)   As to claim 105, the combination of Daniels, Kobata and Jones discloses

the computer implemented method of claim 100, wherein Jones discloses determining

the decryption capability of each recipient in the list of recipients as addressed above in

claim 100. However Jones is silent on the capability of selecting one decryption

capability in accordance with a recipient's preference if the recipient has more than one

decryption capability. Daniels discloses a message router delivers the electronic mail in

accordance with recipient's delivery preference, those delivery preferences may be an

electronic mail address, a pager, a facsimile machine and a printer (see Daniels: col. 2,

lines 14-17), the concept of selecting the delivery mechanism in accordance with a

recipient's preference if the recipient has more than one delivery preference can be

implemented for decryption capability so as to accommodate recipients with several

different decryption capabilities.

8.   Claims 101-102 and 106-107 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Daniels, Jr. et al. (6,343,327) in view of Kobata et al. (7,051,003) in

view of Jones et al. (6,697,944) and further in view of Bengtsson et al. (6,865,191).

        a)   As to claim 101, the combination of Daniels, Kobata and Jones discloses

the method of claim 100 further comprising notifying the recipient that the message is

available for retrieval (i.e. the sending system notifies the receiving system of the

imminent delivery of a parcel, see Kobata: col. 5, lines 43-46), however it is silent on the

capability of disclosing for each recipient that does not have decryption capability or the

decryption capability can not be determined, (notifying the recipient that the message is

available for retrieval). Bengtsson is relied on for the teaching of having for each

recipient that does not have decryption capability or the decryption capability cannot be

determined, (notifying the recipient that the message is available for retrieval) (i.e. when

the sender transmit an attachment that the receiver's terminal does not have the

capability to decipher, the server is negotiated to deliver the message in a format that is

understood by the receiver's terminal. If the recipient does not have a terminal, then the

attached file could be accessed through the Internet, see Bengtsson: col. 6, lines 60-67). It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of having for each recipient that does not have decryption capability or the decryption capability cannot be determined in the system of Daniels, Kobata and Jones, as Bengtsson teaches, so as to properly inform the recipient of the transmitted message.

b)   As to claim 102, the combination of Daniels, Kobata, Jones and Bengtsson discloses the computer implemented method of claim 101, wherein notifying the recipient includes notifying the recipient that the message is available for retrieval through a secure link (i.e. the retrieval can require log-on authentication such as username and password to retrieve message, see Kobata: col. 6, lines 34-45).

c)   As to claim 106, Daniels discloses a computing system for providing secure message services for messages addressed to multiple recipients (i.e. a system and method for electronic and physical mass mailing, see Daniels: col. 1, lines 5-7) comprising: a forwarding engine (i.e. message router, see Daniels: Fig. 1, element 112) executing on a computer operable to: receive an encrypted message and a list of recipients (i.e. printstream processor 102 may encrypt the documents with a content encryption processor, see Daniels: col. 3, lines 53-55; the encrypted information is forwarded to the message router, see Daniels: Fig. 1, element 112; Daniels discloses a system for mass mailing delivery with addressing information in the form of delivery preferences for each recipients, see Daniels: Fig. 1, element "Control Info. And

References" and col. 4, lines 46-49); deliver the message to the recipient (i.e. the

message router delivers the electronic mail pieces, see Daniels: col. 2, lines 14-17).

Daniels is silent on the capability of decrypting the encrypted message,

determining a decryption capability for each recipient in the list of recipients, for each

recipient, re-encrypting the decrypted message according to the decryption capability of

the recipient and for each recipient that does not have a decryption capability, notify the

recipient that the message is available for retrieval. Kobata is relied on for the teaching

of decrypting the encrypted message, re-encrypting the decrypted message and

delivering the re-encrypted message to the recipient (i.e. a server system is connected

to the network to receive the encoded document, the server system comprises a

processor that executes decryption software to decode the document encoded by the

sending system and executes encryption software to encode the decoded document

before delivering the document, see Kobata: col. 2, lines 40-46).

It would have been obvious to one of ordinary skill in the art at the time of the

invention to employ the use of decrypting the message and re-encrypting the message

in the system of Daniels, as Kobata teaches so as to provide security of the outgoing

electronic mail piece (see Daniels: col. 4, lines 23-25).

The combination of Daniels and Kobata is silent on the capability of determining

a decryption capability for each recipient in the list of recipients and (re-encrypting) the

decrypted message according to the decryption capability of the recipient and for each

recipient that does not have a decryption capability, notify the recipient that the

message is available for retrieval. Jones is relied on for the teaching of determining a

decryption capability for each recipient in the list of recipients and (re-encrypting) the decrypted message according to the decryption capability of the recipient (i.e. digital content is encrypted and transmitted to each portable player device according to the decryption capability of each portable player device, see Jones: col. 4, lines 30-35).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of determining a decryption capability for each recipient in the list of recipients and (re-encrypting) the decrypted message according to the decryption capability of the recipient in the system of Daniels and Kobata, as Jones teaches, so as to ensure proper protection of the transmitted data (see Jones: col. 1, lines 8-14).

Kobata further discloses notifying the recipient that the message is available for retrieval (i.e. the sending system notifies the receiving system of the imminent delivery of a parcel, see Kobata: col. 5, lines 43-46), however the combination of Daniels, Kobata and Jones is silent on the capability of each recipient that does not have a decryption capability, (notify the recipient that the message is available for retrieval)

Bengtsson is relied on for the teaching of having for each recipient that does not have decryption capability or the decryption capability cannot be determined, (notifying the recipient that the message is available for retrieval) (i.e. when the sender transmit an attachment that the receiver's terminal does not have the capability to decipher, the server is negotiated to deliver the message in a format that is understood by the receiver's terminal. If the recipient does not have a terminal, then the attached file could be accessed through the Internet, see Bengtsson: col. 6, lines 60-67). It would have

been obvious to one of ordinary skill in the art at the time of the invention to employ the use of having for each recipient that does not have decryption capability or the decryption capability cannot be determined in the system of Daniels, Kobata and Jones, as Bengtsson teaches, so as to properly inform the recipient of the transmitted message.

d)   As to claim 107, the combination of Daniels, Kobata, Jones and Bengtsson discloses the computing system of claim 106, wherein the forwarding engine is operable to notify the recipient that the message is available for retrieval through a secure link (i.e. the retrieval can require log-on authentication such as username and password to retrieve message, see Kobata: col. 6, lines 34-45).

Conclusion

9.   **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dieu Nguyen whose telephone number is 571-272-3873.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

12.   Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

mdn
9/3/07

CYNTHIA BRITT
PRIMARY EXAMINER
9-4-07